IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF MISSOURI SOUTHWESTERN DIVISION

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
v.	)	Criminal Action
	)	No. 10-05044-01-CR-SW-RED
JASON HILL,	)	
	)	
Defendant.		

REPORT AND RECOMMENDATION OF UNITED STATES MAGISTRATE JUDGE

Pursuant to 28 U.S.C. § 636(b), the above-styled criminal action was referred to the undersigned for preliminary review. This matter comes before the Court on defendant's Motion to Suppress Evidence. The government has responded.

Defendant asserts that evidence seized as a result of the search and seizure of his computers, both with and without a warrant, should be suppressed. He contends that there was a warrantless search made of his computer by the use of a version of E-Phex, "an innovative undercover investigative software [which] allows for a direct connection to a suspect computer from a remote location." [Defendant's Motion to Suppress, at 1]. It is defendant's argument that this constituted warrantless hacking of his computer, resulting in the review of a file list, and the downloading and seizure of a selected number of the file list. Defendant asserts that the material seized from the warrantless computer search was then placed in a sworn affidavit, which was used to secure a search warrant for his residence. His computers were then physically seized and searched pursuant to the search warrant, and items of alleged child pornography were seized. It is his contention that the search and seizure violated the Fourth Amendment because the search with innovative software was not supported by any exception that allows for warrantless searches. Defendant argues that this was

"unauthorized hacking in every sense of the word." Defendant's Motion, at 2. He contends that innovative technology to obtain information can clearly implicate the Fourth Amendment, citing Kyllo v. United States, 533 U.S. 27 (2001). It is also his position that there was no probable cause to support the subsequent search warrant other than the information gleaned through the illegal warrantless search. Therefore, he seeks suppression of all items of alleged contraband secured from the August 3, 2010 warrantless search, and the search pursuant to the warrant issued on September 23, 2010.

It is the government's position that Task Force Officer ["TFO"] James Smith's use of Undercover Investigative Software ["UIS"] to allow him access to an IP address that was utilizing E-Phex, a peer to peer network site, did not implicate a Fourth Amendment right to privacy. The government submits that defendant's contention has been rejected by case law, and that TFO Smith legally used defendant's E-Phex peer to peer network, which he had voluntarily placed on his computer, to access the Gnutella network and to obtain the files that defendant had made available for other users on the network to download. It is argued that defendant installed E-Phex free software on his computer, which allowed access to Gnutella's peer to peer file sharing programs; that he then made files on his computer available for sharing under the Gnutella network through E-Phex. The government states that TFO Smith would never had been able to use the UIS to access defendant's child pornography files through E-Phex and Gnutella if defendant had not provided voluntary access.

Although the Supreme Court has not addressed the issue of peer to peer file sharing in the Fourth Amendment context, it has held, in a consistent line of cases, that individuals have no reasonable expectation of privacy in information exposed to the public or shared with third parties. See, e.g, United States v. Miller, 425 U.S. 435 (1976); Katz v. United States, 389 U.S. 347 (1967).

Courts in various jurisdictions have addressed the issues defendant presents and have determined that defendants have no Fourth Amendment privacy rights in computer files that they have shared on file-sharing networks such as Gnutella. See, e.g., United States v. Gabel, 2010 WL 3927697 (S.D.Fla. 2010); United States v. Stults, 575 F.3d 834 (8th Cir. 2009), cert. denied, –U.S. –, 130 S.Ct. 1309 (2010); United States v. Ganoe, 538 F.3d 1117 (9th Cir. 2008), cert. denied, –U.S.–, 129 S.Ct. 1122 (2009); United States v. Perrine, 518 F.3d 1196 (10th Cir. 2008), cert. denied, –U.S.–, 131 S.Ct. 440 (2010). "There is no reasonable expectation of privacy in computer files that are accessible to users of a computer network." Stults, 575 F.3d at 840. Therefore, based on Eighth Circuit law, the warrantless downloading of files from defendant's computer by law enforcement did not implicate Fourth Amendment concerns. Defendant has cited no case on this specific issue, and the Court finds Kyllo to be non-persuasive where there is ample case law on point. Accordingly, defendant's argument that Officer Smith violated his right to privacy by using the UIS to examine the peer to peer network site E-Phex, which defendant had already elected to voluntarily share with other users, is without merit. Further, defendant's argument that the search warrant lacked probable cause under the "fruits of the poisonous tree" doctrine is also without merit, given that the information relied on by the issuing judge was legally obtained and established probable cause for the issuance of the search warrant.

For the foregoing reasons, it is, pursuant to the governing law and in accordance with Local Rule 72.1 of the United States District Court for the Western District of Missouri,

RECOMMENDED that defendant's Motion to Suppress Evidence be denied.

/s/ James C. England
JAMES C. ENGLAND
United States Magistrate Judge

Date: 6/18/12